ORDER FOR SUPPLIES OR SERVICES (FINAL)

N65236-13-D-5823	0004	2014 Sep 30	N65236-14-NR-55580	DO-A7

6. ISSUED BY	CODE N65236	7. ADMINISTERED BY	CODE S0107A	8. DELIVERY FOB

6. ISSUED BY (CODE N65236)
SPAWAR-Systems Center Lant (CHRL)
P.O. BOX 190022
North Charleston SC 29419-9022

7. ADMINISTERED BY (CODE S0107A)
DCMA HUNTSVILLE
1040 Research Blvd Ste 100
Madison AL 35758-2040

8. DELIVERY FOB
- DESTINATION
- OTHER
- (See Schedule if other)

9. CONTRACTOR (CODE 0A168)   FACILITY
SENTAR INC
315 WYNN DR, STE 1
HUNTSVILLE AL 35805-1960

10. DELIVER TO FOB POINT BY (Date)
See Schedule

11. X IF BUSINESS IS
X	SMALL
	SMALL DISADVANTAGED
X	WOMEN-OWNED

12. DISCOUNT TERMS
Net 30 Days
WIDE AREA WORK FLOW

13. MAIL INVOICES TO THE ADDRESS IN BLOCK
See Section G

14. SHIP TO (CODE)
See Section D

15. PAYMENT WILL BE MADE BY (CODE HQ0338)
DFAS Columbus Center, South Entitlement Operations
P.O. Box 182264
Columbus OH 43218-2264

MARK ALL PACKAGES AND PAPERS WITH IDENTIFICATION NUMBERS IN BLOCKS 1 AND 2.

16. TYPE OF ORDER

DELIVERY/CALL	X	This delivery order/call is issued on another Government agency or in accordance with and subject to terms and conditions of numbered contract.
PURCHASE		Reference your _____ furnish the following on terms specified herein.
		ACCEPTANCE. THE CONTRACTOR HEREBY ACCEPTS THE OFFER REPRESENTED BY THE NUMBERED PURCHASE ORDER AS IT MAY PREVIOUSLY HAVE BEEN OR IS NOW MODIFIED, SUBJECT TO ALL OF THE TERMS AND CONDITIONS SET FORTH, AND AGREES TO PERFORM THE SAME.

SENTAR INC

Bridget Abashian
President and CEO

NAME OF CONTRACTOR	SIGNATURE	TYPED NAME AND TITLE	DATE SIGNED (YYYYMMDD)

If this box is marked, supplier must sign Acceptance and return the following number of copies:

17. ACCOUNTING AND APPROPRIATION DATA/LOCAL USE
See Schedule

18. ITEM NO.	19. SCHEDULE OF SUPPLIES/SERVICES	20. QUANTITY ORDERED/ ACCEPTED *	21. UNIT	22. UNIT PRICE	23. AMOUNT
	See Schedule				

*If quantity accepted by the Government is same as quantity ordered, indicate by X. If different, enter actual quantity accepted below quantity ordered and encircle.	24. UNITED STATES OF AMERICA	25. TOTAL	$4,813,805.95
	BY: /s/Theodore Rivera 09/30/2014 CONTRACTING/ORDERING OFFICER	26. DIFFERENCES	

27a. QUANTITY IN COLUMN 20 HAS BEEN

INSPECTED	RECEIVED	ACCEPTED, AND CONFORMS TO THE CONTRACT EXCEPT AS NOTED:

b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	c. DATE	d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	28. SHIP NO.	29. D.O. VOUCHER NO.	30. INITIALS
	PARTIAL	32. PAID BY	33. AMOUNT VERIFIED CORRECT FOR
f. TELEPHONE g. E-MAIL ADDRESS	FINAL		
36. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT.	31. PAYMENT COMPLETE		34. CHECK NUMBER
a. DATE b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	PARTIAL		35. BILL OF LADING NO.
	FULL		

37. RECEIVED AT	38. RECEIVED BY (Print)	39. DATE RECEIVED	40. TOTAL CON-TAINERS	41. S/R ACCOUNT NUMBER	42. S/R VOUCHER NO.

DD FORM 1155, DEC 2001   PREVIOUS EDITION IS OBSOLETE.

CONTRACT NO.	DELIVERY ORDER NO.	PAGE	FINAL
N65236-13-D-5823	0004	2 of 2	

GENERAL INFORMATION

Page left blank intentionally.

SECTION B SUPPLIES OR SERVICES AND PRICES

CLIN - SUPPLIES OR SERVICES

For Cost Type Items:

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
1001	R425	Integrated Cyber Operations (ICO) Services and solutions in support of mission capabilities within the ICO Portfolio missionareas in accordance with the Performance Work Statement (PWS) contained herein. (Fund Type – TBD)	1.0	LO	(b)(4)	(b)(4)	$4,813,805.95
2001	R425	Integrated Cyber Operations (ICO) Services and solutions in support of mission capabilities within the ICO Portfolio missionareas in accordance with the Performance Work Statement (PWS) contained herein. (Fund Type – TBD)	1.0	LO	(b)(4)	(b)(4)	(b)(4)

Option

SECTION C DESCRIPTIONS AND SPECIFICATIONS

TASK ORDER (TO) PERFORMANCE WORK STATEMENT (PWS)

SPACE AND NAVAL WARFARE SYSTEMS CENTER, ATLANTIC (SSC LANT)

SHORT TITLE: MCNOSC FY14-FY16 Cyber Support

1.0 PRIMARY PLACES OF PERFORMANCE

a. Marine Corps Base Quantico, VA *(primarily)*
b. Contractor facilities
c. SPAWARSYSCEN Atlantic locations

2.0 TASK ORDER PURPOSE

This task order provides cyber support to the Marine Corps Network Operations and Security Center (MSNOSC) and the Marine Corps Enterprise Network (MCEN). The Contractor will support Enterprise Directory and Messaging (EDM) in Active Directory (AD), messaging, virtualization, storage area network (SAN), event management, and database support. The Contractor will provide Integrated Network Support (INS) and web content filtering at the Tier III level. The Contractor will provide vulnerability management, as well as certification and accreditation support with the Compliance and Quality Assurance (CQA) team. The Contractor will mature the capabilities of the MCEN Event Management System (MEMS) by designing, architecting, and implementing increased capabilities within the MEMS toolset.

2.1 BACKGROUND

The Marine Corps is working to unify the MCEN's disparate networks inclusive of tactical, legacy, SIPRNET, and former Navy Marine Corps Intranet into a tightly integrated, agile, defensible, survivable network capable of supporting highly distributed operations as well as an efficient and effective business enterprise. The unified MCEN will be disciplined in its operation ensuring defense against an ever increasing threat and providing the IT services and service support needed to meet the operational flexibility Marine Forces provide the Nation. Key to this effort is a centralized network management strategy and tool set with standard constructs to reduce overhead and increase effectiveness and efficiencies in network operations.

The MCNOSC is an operational organization responsible for the operation and defense of the Marine Corps Enterprise Network (MCEN). The MCNOSC maintains the responsibility for the execution of current and emerging Department of Defense (DoD) Information Security (IS) and Information Assurance (IA) doctrine as well as promulgation of Marine Corps specific policies and procedures outlining the protection of all information communication mediums. The MCNOSC implements and enforces policies and NetOps directives, orders and procedures under the administrative and operational control of Marine Forces Cyberspace Command (MARFORCYBER).

The MCEN, at the lowest level, provides connectivity for Microsoft Windows servers, clients, Transmission Control Protocol/Internet Protocol (TCP/IP) hosts and clients in a tactical environment, aboard ships or on a base, deployed camps and stations. At its highest tier, the network consists of interconnected Integrated Digital Network Exchange (IDNX) trunk circuits routing TCP/IP, and, in some cases, System Network Architecture (SNA) protocols. Regional access to the Defense Information System Network (DISN) and its component networks, such as, the Non-secure Internet Protocol Routed Network (NIPRNET), and the Secret Internet Protocol Routed Network (SIPRNET) is also provided by the network at its highest tier.

2.2 SCOPE

The MCNOSC Cyber Support task order provides cyber support to the Marine Corps Network Operations and Security Center (MCNOSC) and the Marine Corps Enterprise Network (MCEN). The Contractor will support Enterprise Directory and Messaging (EDM) in Active Directory (AD), messaging, virtualization, storage area network (SAN), event management, and database support. The Contractor will provide Integrated Network Support (INS) and web content filtering at the Tier III level. The Contractor will provide vulnerability management, as well as certification and accreditation support with the Compliance and Quality Assurance (CQA) team. The Contractor

will mature the capabilities of the MCEN Event Management System (MEMS) by designing, architecting, and implementing increased capabilities within the MEMS toolset.

The tasking is broken into three sub-sections which effectively provide four separate teams in support of the MCNOSC:

1. Enterprise Directory and Messaging (EDM)

2. Integrated Network Support (INS)

3. MCEN Event Management System (MEMS) Support

4. Compliance & Quality Assurance (CQA) Support

3.0   APPLICABLE DOCUMENTS

3.1   REFERENCES

All references listed within the basic contract are required as applicable to this TO.

3.2   SPECIFICATIONS

All specifications listed in the basic contract are applicable as required by this TO.

- DoD 8570
- DoD 8500
- DISA CIRCULAR 300-115-3
- DISA STIGS
- MCNOSC Desktop Procedure D03-502
- MCNOSC Order 3100 (CCIR)
- MCNOSC Order 3020.1 (COOP)
- Headquarters Marine Corps, C4, Enterprise Security Directives
- DISA Connection Approval Process (DISA CAP)
- DISA Circulars
- INS Desktop Procedures and policies

4.0   SECURITY REQUIREMENTS

The required minimum security clearance for each task order activity is indicated in the table below.

Task Order Activity Paragraph	Required Minimum Security Clearance
TO Paragraph 6.1, 6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.1.5, 6.1.6, 6.2, 6.2.1, 6.2.1.1 6.3	Secret
TO Paragraph 6.4, 6.4.1, 6.4.2	Top Secret

Clearance is required to access and handle classified and personal personnel material, attend program meetings, and/or work within restricted areas unescorted. Access to SCI will be limited to U.S. Government Facilities or other U.S. Government sponsored SCI Facilities (SCIFs) authorized in accordance with the DD254. Generation of SCI deliverables is not authorized.

The Contractor shall be required to comply with all Marine Corps installation rules and regulations applicable to the conduct, safety, security, and procedures governing site entry and exit. The Contractor shall be proficient on all of the systems and applications that are employed at the command. All Contractor support staff must be U.S. citizens and those requiring access to the Customer site must possess an appropriate security clearance as stated herein.

4.1   ORGANIZATION

As specified in clause 5252.204-9200 and the Contract Security Classification Specification form, DD-254, classified work shall be performed under this task order. The Contractor shall have at time of TO award a TOP SECRET facility security clearance (FCL). Generation of SCI deliverables is not authorized.

4.2   PERSONNEL

Prior to commencement of work on this contract, all Contractor personnel (including administrative and subcontractor personnel) shall have, at a minimum, a favorable Trustworthiness Determination, which is determined by a National Agency Check with Local Agency Check and Credit Check (NACLC) favorable FBI fingerprint checks. Some personnel shall possess a TOP SECRET clearance with Single Scope Background Investigation (SSBI) prior to working on TO.

The labor for the task order activities below require personnel security clearances as indicated in the table.

Task Order Activity Paragraph	Required Minimum Security Clearance
TO Paragraph 6.1, 6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.1.5, 6.1.6, 6.2, 6.2.1, 6.2.1.1 6.3	Secret
TO Paragraph 6.4, 6.4.1, 6.4.2, 6.4.3	Top Secret

5.0   COR DESIGNATION

The Contracting Officer Representative (COR) for this task order is [(b)(6)   ], 54500 who can be reached at phone (540) 220-(b)(6); e-mail: [(b)(6)   ]

6.0   DESCRIPTION OF WORK

The Contractor is responsible for and shall support a broad range of technical and operational functions in support of MCNOSC.

The percentage of work associated with this task activity may vary slightly by program precedent and volume throughout the performance period. The Contractor is responsible for providing suitable technical and analytical expertise to support ongoing responsibilities delineated by activity, as well as variances in the scope of activities. The Contractor shall appoint a technical manager to act as both coordinator of task activities and to serve as the overall expert for successful completion of this task initiative. Administrative support shall be provided as required. (A003)

6.1   ENTERPRISE DIRECTORY AND MESSAGING

Enterprise Directory and Messaging (EDM) consist of five groups of technologies that are associated with all the services it provides. The services, also called Product Groups (PGs), include Messaging, Platforms, Virtualization and SAN, Event and Configuration Management, and Defense Messaging System (DMS). Within each PG there are numerous technologies and services designed, managed, and operated by EDM.

6.1 .1   PROJECT OVERSIGHT

The contractor shall accomplish the specific management and engineering tasks described in the following paragraphs utilizing the SSC Atlantic Integrated Product Team (IPT) approach coupled with a proven, disciplined and streamlined Systems Engineering process. Expected reports include Task Order Status Report, Contractor's Manpower Report, Task Order Closeout Report, , Cost and Milestones Schedule Plan, Contractor CPARS Draft Approval Document (CDAD) Report Cyber Security Workforce (CSWF) Report, Provide INS Reporting - Tier III Meetings, Enterprise-wide Contractor manpower reporting application (eCMRA) input. Invoice Support Documentation, Limitation Notification & Rationale, (CDRL A003, A004, A005, A007, A008, A009, A011, A012, T001, T002, T003)

CDRL A015: A Contractor Manpower Quarterly Status Report shall be provided to the government four times throughout the calendar year. Required for all active service contracts, beginning at the time of contract award, the Manpower report shall itemize specific contract and/or TO administrative data as specified in the applicable DD

1423 form. Utilizing a format provided by the government, the contractor shall collect required data throughout the specified performance period and shall submit one cumulative report on the applicable quarterly due date.

Enterprise-wide Contractor Manpower Reporting Application

CDRL T001: The contractor shall report all contractor labor hours (including subcontractor labor hours) required for performance of services via a secure data collection website – Enterprise-wide Contractor Manpower Reporting Application (eCMRA). The contractor is required to completely fill-in all required data fields using the following web address: http://www.ecmra.mil/.

Reporting inputs shall be for the labor executed during the period of performance during each Government fiscal year (FY) which runs from October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year, beginning with 2013. Contractors may direct questions to the help desk at http://www.ecrma.mil/ <http://www.ecrma.mil/>.

6.1.2   EDM Active Directory (AD) Support

The EDM AD Support team supports over 255,000 user accounts across several AD forests on USMC's operated networks. The services the AD Support team supports in Active Directory include accounts and group management, security, Windows Internet Name Service, Domain Name Service, Dynamic Host Configuration Protocol, File Replication Service, Group Policy Object's and other directory services technologies as applicable.

The Contractor shall possess recent and relevant experience with Active Directory at the Tier II and III level and utilize their knowledge of the Windows Server Operating System and applications that are supported by Active Directory to provide EDM AD support. The environment is VMware based and requires the Contractor to use its knowledge in VMware Virtualization, applicable certifications (e.g., VMware VCP) and VMware vCloud to perform the specialized EDM Active Directory tasks.

<u>The Contractor shall provide the following services to support EDM Active Directory tasks</u>:

- Resolve all Active Directory tickets escalated from the service desk.
- Provide guidance and instruction to the service desk for handling standard Active Directory related incidents and service requests.
- Provide Active Directory Service Desk Resolution Reports documentation to the service desk on the procedures for completing the task.
- Submit and execute AD related Request for Change (RFC) tasks.
- Maintain the overall health of technologies associated with AD.
- Monitor the health of AD with MCNOSC-provided event management tools and make corrective actions to incidents that lower the health of AD.
- Provide MCNOSC project support for AD related technologies.
- Coordinate with S5 and other MCNOSC sections on AD-related issues.
- Participate in the Change Review Board.
- Escalate issues to third party product vendors.
- Follow all ITIL version 3.0 (and later versions) processes as they are applied to the MCNOSC.
- Implement monitoring tool thresholds and conduct proactive event remediation.

6.1.3   EDM Messaging Support

The Contractor shall configure all aspects of the Microsoft Enterprise Exchange (Exchange Server) organization in support of a 255,000 user environment across all AD forests on USMC operated networks to provide messaging support.

The Contractor shall use its experience with Exchange Server at the Tier II and III level to provide EDM messaging services. This includes exposure to firewalls as they relate to Exchange, Outlook, OWA, BES, message routing, Database Management, and AV/Hygiene applications utilized by Microsoft Exchange.

The Contractor shall use its experience with VMware Virtualization, VMware vCloud, messaging including Mailbox Servers, Hub Transports, Outlook Web Access, Blackberry Enterprise Server (BES) Integration and Public Key Infrastructure (PKI) <u>perform the following EDM messaging tasks</u>:

- Resolve all EDM messaging tickets escalated from the service desk and provide an EDM Messaging Status Report on a weekly basis to MCNOSC TPOC or designee.
- Provide Directory Support for the following products: ADAM, SimpleSync, and Identity Integration Feature Pack
- Manage the USMC Global Address List (GAL).
- Configure Antivirus products and Host-Based Security System (HBSS) as they relate to Exchange Servers.
- Provide guidance and instruction to the service desk for handling standard Message related incidents and service requests.
- Provide EDM Message documentation to the service desk on the procedures used to completing the task.
- Submit and execute Message related Request for Change (RFC) tasks.
- Escalate message incident tickets to Tier III and other sections.
- Maintain the overall health of technologies associated with Messaging.
- Monitor the health of Messaging with MCNOSC-provided event management tools.
- Provide MCNOSC project support for Messaging related technologies.
- Coordinate with S5 and other MCNOSC sections on EDM messaging issues.
- Participate in a Change Review Board.
- Escalate issues to third party product vendors.
- Follow all ITIL v 3.0 processes (and later versions) as they are applied to the MCNOSC.
- Implement monitoring tool thresholds and conduct proactive event remediation.
- Ensure that any latency, whether at the Command or the Forward Operating Bases (FOBs) level, is quickly identified and mitigated/remediated upon discovery.
- Maintain a "forward looking" posture and work with the MCNOSC management to plan for future upgrades, including Exchange migration to the newer versions.

6.1.4 EDM Virtualization Support (VM)

The Contractor shall configure all aspects of Virtualization in support of a 255,000 user environment across all forests on USMC operated networks. The Contractor shall use its experience with VMware and the experience to deploy and maintain complex VMware environments to provide virtualization services.

The Contractor shall use its experience with VMware Update Manager, VSphere, ESXi, storage area networks, SnapManager, Windows Server operating systems, VMware vCloud and DISA Standard Technical Implementation Guidance compliancy to provide Virtual Machine services. The Contractor shall work with customers and vendors on configuration of features and functionality; train and mentor junior administrators in best practices and internal processes; assist with change management and documentation of environments; work with a dedicated team to ensure success of select customer groups; and ensure customer uptime through precise monitoring implementations, good change management, and incorporation of best practices.

<u>The Contractor shall provide the following EDM virtualization support services</u>:

- Resolve all EDM VM tickets and provide an EDM VM Status Report on a weekly basis to the MCNOSC TPOC or designee for incidents escalated from the service desk.
- Provide guidance and instruction to the service desk for handling standard virtual infrastructure (VI) related incidents and service requests.
- Provide EDM Virtual Machine documentation to service desk on the procedures for completing the task.
- Submit and execute VI related Request for Change (RFC) tasks.
- Escalate EDM Virtual Machines tickets to Tier III and other sections.
- Maintain the overall health of technologies associated with Virtual Infrastructure.
- Monitor the health of VI with MCNOSC provided event management tools.
- Provide MCNOSC project support for VI related technologies.
- Coordinate with S5 and other MCNOSC sections on EDM VM issues.
- Participate in a Change Review Board.
- Escalate issues to third-party product vendors.
- Follow all ITIL Version 3.0 (and later versions) processes as they are applied to the MCNOSC.
- Implement monitoring tool thresholds and conduct proactive event remediation.
- Guide MCNOSC towards a highly flexible, extensible and cost-effective Virtual Cloud Infrastructure.

6.1.5   EDM Storage Area Network (SAN) Support

The Contractor shall configure all of the aspects of the Storage Area Network (SAN) hardware and software within the MCNOSC installation.   The Contractor shall use its experience with SAN to include Snaps, storage provisioning, management software, recovery procedures, hardware installation and security of Logical Unit Numbers (LUNS) and access to each to provide EDM SAN support.

The Contractor shall use its knowledge of Storage filers, software and hardware at the Tier III Level and its expertise with Windows, VMware, and networking to provide EDM SAN services. The environment is VMware based and the Contractor shall use its knowledge of VMware to provide SAN services.

<u>The Contractor shall provide the following EDM SAN services</u>:

- Resolve all EDM SAN tickets and provide an EDM SAN Status Report on a weekly basis for all SAN incidents escalated from Tier I organizations.
- Provide guidance and instruction to the Tier I organizations for handling standard SAN related incidents and service requests.
- Provide EDM SAN documentation to Tier I organizations on the procedures for completing the task.
- Submit and execute SAN related Request for Change (RFC) tasks.
- Escalate EDM SAN incident tickets to Tier III and other sections.
- Maintain the overall health of technologies associated with Storage Area Networks.
- Monitor the health of SANs with MCNOSC- provided event management tools.
- Provide MCNOSC project support for SAN related technologies.
- Coordinate with S5 and other MCNOSC sections on EDM SAN issues.
- Participate in a Change Review Board.
- Escalate issues to third party product vendors.
- Follow all ITIL version 3.0 (and later versions) processes as they are applied to the MCNOSC.
- Implement monitoring tool thresholds and conduct proactive event remediation.
- Work closely with the MCNOSC management to continually improve the SAN performance while recommending solutions that reduce the overall Total Cost of Ownership (TCO) and increase the MCNOSC Return on Investment (ROI) on the SAN investment.

6.1.6   EDM Event Management Support

The Contractor shall support the Systems Center Operations Manager (SCOM) role in installations. The Contractor shall install Management Servers, Agents, reporting servers, and data warehouses where necessary and configure rules and alerts consistent with the support structure.

The Contractor shall use its experience with Microsoft Operations Manager (MOM) or SCOM, ISA/TMG Server, Active Directory, firewalls and other network management tools at the Tier III level to provide EDM Event Management Support. The Contractor shall use their expertise with Windows Server, Exchange, networking, PKI and SSL and support of the products for the EDM Management Support. The environment is VMware based and requires the Contractor's knowledge of VMware to provide Event Management services.

<u>The Contractor shall provide the following EDM Event Management services</u>:

- Resolve all Event Management tickets and provide an Event Management Status Report on weekly basis for all Event Management incidents escalated from the Tier I organizations.
- Provide guidance and instruction to Tier I organizations for handling standard Event Management related incidents and service requests.
- Provide Event Management documentation to Tier I organizations on the procedures for completing the task.
- Submit and execute Event Management related Request for Change (RFC) tasks with approval of Government designated TPOC.
- Escalate Event Management tickets to Tier III and other sections.
- Maintain the overall health of technologies associated with Event Management.
- Monitor the health of Event Management Infrastructure with MCNOSC provided event management tools.
- Provide MCNOSC project support for Event Management related technologies.
- Coordinate with S5 and other MCNOSC sections on Event Management issues.
- Participate in a Change Review Board.

- Escalate issues to third party product vendors.
- Follow all ITIL v 3.0 (and later versions) processes as they are applied to the MCNOSC.
- Implement monitoring tool thresholds and conduct proactive event remediation.

6.1.7   EDM Database Support (DBA)

The Contractor shall configure and operate Microsoft SQL databases to include Oracle, throughout USMC application servers in a secure manner. The Contractor shall configure SSL access and logging on the devices.

The Contractor shall use its experience with Database management at the Tier II and Tier III level and expertise with Clustering, Disaster Recovery, Scripting and Reporting Services to provide EDM DBA. The Contractor shall use its industry certifications commensurate with the level of expertise required for the tasks (e.g., Microsoft MCDBA, etc.) to provide DBA services. The system environment is VMware based and the Contractor shall use its knowledge of VMware Networking to provide DBA services.

The Contractor shall provide the following EDM DBA support services:

- Resolve all EDM DBA incident tickets and provide a DBA Status Report on a weekly basis on DBA incidents escalated from Tier I organizations.
- Provide guidance and instruction to the service desk for handling standard network infrastructure related incidents and service requests.
- Provide DBA Documentation to Tier I organizations on the procedures for completing the task.
- Submit and execute network related Request for Change (RFC) tasks.
- Escalate DBA tickets to Tier III and other sections.
- Maintain the overall health of technologies associated with Database Infrastructure.
- Monitor the health of Database Infrastructure with MCNOSC provided event management tools.
- Provide MCNOSC project support for Database Infrastructure related technologies.
- Coordinate with S5 and other MCNOSC sections on DBA issues.
- Participate in a Change Review Board.
- Escalate DBA issues to third party product vendors.
- Follow all ITIL v 3.0 (and later versions) processes as they are applied to the MCNOSC.
- Implement monitoring tool thresholds and conduct proactive event remediation.

6.2   INTEGRATED NETWORK SUPPORT

The mission of Integrated Network Support (INS) is to manage the Information Assurance (IA) boundary architecture for the garrison and tactical MCEN while ensuring compliance with the MCNOSC and DISA published technical guidance and higher operational standards; to provide customized on-site training and tactical network support to the Marine Corps Operational Forces; to provide Marine Corps unified capabilities to the Marine Corps Operational Forces to include Voice Over Internet Protocol (VOIP), Voice Over Secure Internet Protocol (VOSIP), and Video Teleconferencing (VTC).

The MCEN consists of tactical networks, networks deployed aboard ships, and garrison networks aboard camps and stations. At its highest tier, the MCEN is interconnected to the Department of Defense (DoD) Information Network (DoDIN), a globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. Regional access to the Defense Information System Network (DISN) and its component networks, such as, the Non-secure Internet Protocol Router Network (NIPRNet), and the Secret Internet Protocol Router Network (SIPRNet) is also provided. The MCNOSC INS, Tier III Section provides Tier III support for approximately 300 classified and un-classified garrison and about 25 deployed tactical Information Assurance (IA) boundary suites around the world and the WAN links that connect those sites to each other and to DISA.

The pace of work in the INS department is very fast in general, supporting a vast array of services running on the MCEN which are depended upon by a diverse community of civilians, Marines, public and private sector agencies and personnel. INS personnel coordinate with other MCNOSC sections to include Enterprise Directory and Messaging (EDM) and The Defense Cyber Operations Section (DCOS), outside Department of Defense (DoD) agencies to include DISA, EA-TJTN, and the other armed services, other Federal Government agencies to include the Department of State, and civilian organizations to include HW and SW vendors such as Cisco, Juniper, McAfee, Riverbed, RedHat, Acme Packet, REDCOM, Avaya and FortiNet.

Unless otherwise supplemented or superseded, directives identified in section 3.2 of this PWS are applicable.

The Contractor shall support the following Hardware and Software platforms within INS:

- Web Content Filtering Support

    o Hardware: BlueCoat

    o Software: BlueCoat

6.2.1 Tier III Integrated Network Support

INS Tier III serves as the Subject Matter Experts for all systems supported by INS. Tier III provides third echelon support for network IA devices to all units MCEN wide and provides escalated technical support to Tier II technicians in the areas pertaining to associated areas of expertise. Tier III also provides planning for MCEN IA boundaries for the installation and configuration of all IA network devices located throughout the MCEN, acting as a two-way conduit by consulting with and providing technical guidance to other MCNSOC sections regarding the testing, planning, and implementation of new network IA devices, as well as facilitating the transition of new capabilities to operations when appropriate. Tier III SME's also assist with the review of external or development of internal policies and plans related to MCEN operations in order to ensure standardization and compliance with NetOps requirements throughout the Marine Corps. (CDRL A012)

The Contractor shall attend weekly Tier III section meetings with Government staff to provide verbal and written updates related to Tier III tasks; problems they have encountered in the past week; and completion plans for the coming week's tasks. The Contractor shall document these Tier III issues and plans in a Tier III INS Weekly Status Report, as defined in the INS Desktop procedures.

6.2.1.1 Web Content Filtering Support Tier III

The Contractor shall use its knowledge and experience with BlueCoat Web Content Filtering devices to <u>provide the following Web Content Filtering support</u>:

- Configure all of the aspects of the Web Content Filter systems within the MCEN IA boundary suites.
- Provide services that include all aspects of Web Content Filtering device operation, configuration, and maintenance.

6.3 MCEN EVENT MANAGEMENT SYSTEM (MEMS) SUPPORT

The MCNOSC will mature the capabilities of the MCEN Event Management System (MEMS) for expanded situational awareness and increased incident and event identification and response capabilities across the Marine Corps Enterprise Network. In order to support these objectives, the MCNOSC will require Contractor support to design, architect, and implement increased capabilities within the MEMs tool set. The government will provide access to existing architecture designs upon contract award. Innovative staffing solutions are encouraged. *The focus of the scope is Design and Architecture Support for the MEMS toolset.*

MEMS support includes design, architecture, and implementation of increased capabilities within the newly implemented enterprise event management tool set on both unclassified and classified enterprise network environments. The tool set is intended to facilitate the Marine Corps' ability to provide IT personnel across the Marine Corps with enhanced ability to monitor and manage the performance and availability of USMC services, systems, networks, and storage. Current components of the USMC MEMS toolset are described as follows;

- MCEN Event Management System (MEMS)
    - HP Enterprise Management Software technologies (listed in detail below) and
    - Microsoft IIS and Apache Tomcat Web Servers and
    - Oracle and SQL Server Relational Database technologies

Key activities associated with MEMS Support include design, architecture, and implementation of capabilities within the HP tool set. <u>General requirements include</u>:

- Enhanced Monitoring capabilities. Deployment of Operations Manager Smart Plug Ins for key USMC IT Services such as Blackberry, Exchange, Active Directory, Database, Middleware, and Virtualization infrastructure services.
- Enhanced UCMDB discovery and mapping. Includes discovery of virtual infrastructure and other services and synchronization of HP BSM to populate the HP Run Time Service Model (RTSM)
- HP tools expertise to support the integration of HP tool set with BMC ITSM tool set, including UCMDB integration with the Atrium CMDB and HP OMi events into BMC Remedy
- Enhanced Service Intelligence, including implementation and configuration of HP Service Health Reporter (SHR) for high level reporting on key MCEN services and infrastructure health. Additionally includes implementation and configuration of HP Service Health Optimizer (SHO) to provide reporting and planning within virtual environments and other USMC IT services.
- Enhanced application monitoring to emulate user experience. Includes implementation and configuration of HP Real User Monitoring (RUM) and diagnostics.
- Enhanced UCMDB discovery including systems, applications, and associated interrelationships and dependencies as well as creation of Service Maps.
- Implementation and configuration of HP Service Intelligence Analyzer (SHA) to provide analysis of Service Health and predictive capabilities in support of Service monitoring and management.
- HP BSM/OMi enhancements to include development and implementation of Topology Based Event Correlation (TBEC) to aid in reducing Mean Time To Repair (MTTR)
- Implementation and configuration of HP Server Automation (SA), Network Automation (NA), and Operations Orchestration to automate functions of deployment, maintenance, configuration management, and, incident response for MCEN Services and infrastructure.
- Author, update, and sustain system design, configuration, and administration documentation
- Provide early life support and assist in promoting adoption of newly implemented MEMS capabilities.

Although the Contractor will be focused on the design, architecture, and implementation of new capabilities and operations and maintenance of the existing implementation, this is not the primary focus; the Contractor will be responsible for ensuring that availability of services is not impacted during the implementation or design of new capabilities. The Contractor will be responsible for responding to and remediating service impacts occurring as a result of design or implementation activities inherent to this contract. The Contractor will also ensure that design, architecture, and implementation activities are conducted in accordance with Original Equipment Manufacturer (OEM) guidelines, MCNOSC SOPs and Local SOP's. In the event of service impact during design or implementation activities, the Contractor will be responsible for adhering to the specified service levels below:

SERVICE LEVEL REQUIREMENTS

Severity Levels:

Severity Level 1	A Severity Level 1 is defined as an: Unclassified network service-impacting outage that meets metric parameters (user / seat size) and also meets any of the following criteria:	· Severity Level 1 is an outage impacting 1,000 or more users or seats, with a duration of twenty (20) minutes. · An entire site which impacts 1 or more VIP or mission-critical seat or individual as defined in the EPMD or Remedy system. · Any High-Interest (HIT) list site. · Any Blackberry, Defense Messaging System (DMS), or pier connectivity issue. · Any high-profile or high-visibility issue that does not meet the above criteria but requires immediate resolution due to

		sensitivity and/or customers impacted.
Severity Level 2	A Severity Level 2 is defined as an: Unclassified Network service impacting outage that meet metric parameters (100 - 999 users or seats,) impacting potentially, (with a duration of twenty (20) minutes or more) which also meets any of the following criteria:	· Any outage for 100-999 users or a High-Interest (HIT) List site. · Any Blackberry, DMS, or Pier Connectivity issue; and high-profile or high-visibility issue that does not meet the above criteria but requires immediate resolution due to sensitivity and/or customers impacted.
Severity level 3	Severity Level-3 is a degradation of any service or affecting any site for which MCNOSC leadership determines there is an elevated visibility. Severity Level will be elevated by MCNOSC direction to Severity Level 2 or Severity Level 1 for resolution.	· Stubbed mailboxes will always require a Severity 3 RtOP (Restore to Operations) report until customer archived mail is restored. NOTE: Power outages do not require a RtOP unless it is a HIT list site or service.

#	Required Service	Details	Performance Standard
1	On-Call Response Time	Average response times required of personnel on-call.	Objective =< 15 Min Threshold =<1 hr
2	Recovery Time Objective	Establish LOS for Recovery Time Objective (RTO) for service recovery in accordance with (time to restore):	Threshold: 8 hour, normal business hours. Objective: 4 hours, normal business hours.
3	Recovery Point Objective	Establish Level of Service for Recovery Point Objective (RPO) for recovery of data in accordance with (acceptable loss):	Threshold: 24 hours, 1 business day, in accordance with normal business hours. Objective: 8 hours, normal business hours.
4	Storage Usage	Monitor overall storage usage will not surpass 70%, leaving 30% capacity available Time Interval:	Measured once every 24 hours, summarized weekly, and reported monthly
5	Average Time to Resolve Severity Level 1 Incidents	Average response time to resolve Severity 1 incidents.	Objective = <8hrs. Provide updates every 90 minutes until resolution.
6	Average Time to Resolve Severity Level 2 Incidents	Average response time to resolve Severity 2 incidents.	Objective = <24hrs. Provide updates every 12 hours until resolution.
7	Measuring Successful Problem Resolution.	The formula for the closed incidents is the number of closed incidents completed within the required target values / total number of incidents. All measurements are based on a 24	Threshold: 4 hrs > 80.0%, 4 days > 90.0%, 14 days > 99.0%. Objective: 2 hrs > 90.0%, 1 day > 99.0%.

		hours a day/7 days a week operation.	
8	Incident Repeat Rate	Contractor will effectively ensure that incidents are being analyzed for root cause. If true root causes of problems are being eliminated the incident repeat rate should be a critical metric that shows this.	The incident repeat rate is: <5% incident repeat rate (50,000 dpmo, 3.14 sigma)

6.4   MCEN COMPLIANCE & QUALITY ASSURANCE (CQA)

Due to an increased work load of the MCEN migration, Compliancy and Quality Assurance (C&QA) is requesting additional personnel to ensure mission success.

6.4.1   Vulnerability Management Team (VMT) Support

The Contractor shall assist in developing a plan/capability to audit compliance and discover enterprise security discrepancies, assessing associated risk and assisting in the development of remedial action in coordination with other sections within the MCNOSC if needed, perform detailed analysis in support of OS and Application level vulnerabilities, develop a weekly Vulnerability Assessment Report (VAR), prioritize mitigation actions based on the assessed risk level of critical vulnerabilities discovered /identified from USCC, etc. They shall also develop techniques for tracking and trending enterprise vulnerabilities. (CDRL T004)

6.4.2   Certification & Accreditation (C&A) Support

Develop a framework that provides direction, support, and oversight for Marine Corps C&A and Federal Information Security Management Act (FISMA) compliance, which affects systems and applications throughout the entire Marine Corps. This effort works with all Marine Corps organizations, locations, and commands to ensure all systems and applications meet security requirements cradle to grave.

The Contractor shall assist the MCNOSC in supplying system security engineering reviews, to include system security evaluations, security test and evaluation (ST&E) execution and review, support the oversight of MCNOSC Certification & Accreditation (C&A) and FISMA compliance.

Technical Qualifications/Experience: Overall three (2) years of experience in assessing, analyzing, evaluating, validating, certifying and accrediting, etc., various businesses, systems, software development processes, etc., relative to one or more compliance standard, security controls/requirements, etc..

Functional Responsibility: Responsible for evaluating various businesses, systems, software development processes, etc., validating against standard requirements and/or compliance controls, e.g., ISO, CMMI, HIPAA/HITECH, NIST, DIACAP, DODIIS/DCID, CNSS, ICD 503, etc. Responsible for assisting in the scoping effort relative to the target compliance activity. Assist in the development of the compliance methodology based on experience as well as best practices associated with target compliance activity. Document tasks to justify compliance, bring target into compliance (both technically and non), and present compliance package for approval by clients and/or approval chains as is appropriate. Analyze and evaluate the security requirements/controls in an organization, validating them with standard security guidelines and policies, and certifying that all information systems are compliant with standard security guidelines.

Specific Contractor duties will be:

- Security review of system requirements to evaluate general system, DADMS/DITPR-DON ID, and FISMA reportable information
- Security review of DIP to evaluate information assurance (IA) controls in relation to DOD 8500.2 and/or NIST 800-53 requirements
- Security review of system information and inventory to evaluate IA controls (DOD 8500.2 and/or NIST 800-53) as approved by the AO
- System Security Review of IV&V Test Plan in accordance with applicable STIGS/SRGs/Checklists
- System Security Review of IV&V Results in accordance with the AO approved DIP
- System Security Review of POA&M in accordance with IV&V findings and associated status of

vulnerabilities
- System Security Review of Remedy Trouble Tickets associated to Requests for Modification/Information /Troubleshooting
- System Security Review of Ports, Protocols and Services Registration in accordance with MARADMIN 371-13 and ECSD 021 for final accreditation
- System Security Reviews of USMC C-ISPs in accordance with DoDI 8100.02, CJCSI 6211.02D

Travel, in addition to local travel, will be required on this task as needed in support of the C&A effort, and is estimated in section 10.0 of this PWS. Specific experience/qualification requirements are outlined in section 15.4 of this PWS.

Knowledge Transfer

The SME shall provide informal, hands-on knowledge transfer to representatives selected by MCNOSC on all Certification and Accreditation, VMT and IA activities, and shall occur during the course of the engagement. Knowledge transfer is essentially knowledge sharing between the SME and MCNOSC selected representatives.

7.0   GOVERNMENT FURNISHED INFORMATION (GFI)

No GFI will be provided on this TO.

8.0   GOVERNMENT FURNISHED PROPERTY (GFP)

8.1   GOVERNMENT FURNISHED EQUIPMENT (GFE)

The Government will furnish work spaces, including necessary utilities, electrical power, test data files/forms to accomplish tasks associated with this task order activity. The Government will supply office space, office supplies, computer equipment, telephone, and reproduction, Standard Operation Procedures, applicable regulations, manuals, texts, briefs, and other materials associated with the project and the hardware/software noted throughout this PWS as required. The Contractor shall be responsible for the routine work day care, maintenance, and cleanliness of space provided. The Government will also provide computer resources to support all work areas on an as required and available basis.

8.2   GOVERNMENT FURNISHED MATERIAL (GFM)

No GFM will be provided on this TO.

9.0   CONTRACTOR ACQUIRED PROPERTY (CAP)

9.1   CONTRACTOR ACQUIRED EQUIPMENT (CAE)

No CAE is allowed on this TO.

9.2   CONTRACTOR ACQUIRED MATERIAL (CAM)

No CAM is allowed on this TO.

10.0   TRAVEL

For planning purposes, it is anticipated that the following travel requirements noted below shall be required

# Trips	# People	# Days/Nights	From (Location)	To (Location)
1	10	1/0	Quantico, VA	Columbia, MD
1	4	5/4	Quantico, VA	Camp Pendleton, CA
1	4	5/4	Quantico, VA	Camp Lejeune, NC
1	4	5/4	Quantico, VA	Stuttgart, Germany
1	4	5/4	Quantico, VA	Tampa, FL
1	4	5/4	Quantico, VA	Miramar, CA
1	4	5/4	Quantico, VA	29 Palms, CA

1	4	5/4	Quantico, VA	Norfolk, VA
1	4	5/4	Quantico, VA	San Diego, CA
1	4	5/4	Quantico, VA	Kansas City, MO
1	4	5/4	Quantico, VA	Chambersburg, PA

11.0   TRANSPORTATION OF EQUIPMENT/MATERIAL

No transportation of equipment/material is required on this TO.

12.0   DELIVERABLES

12.1   CONTRACT DATA REQUIREMENTS LIST (CDRL)

12.1.1 Administrative CDRL

As required under TO PWS Para 6.1, the following table lists all required administrative data deliverables, Contract Data Requirements Lists (CDRLs), applicable to this task:

CDRL #	Deliverable Title	TO PWS Reference Para	Frequency	Date Due
A003	Task Order Status Report	6.1.1	MTHLY	30 Days after task order (DATO) and monthly on the 10th
A004	Contractor Manpower Quarterly Status Report	6.1.1	QRTLY	15 Jan, 15 Apr, 15 Jul, & 15 Oct
A005	Task Order Closeout Report	6.1.1	ONE	NLT 30 days after completion date
A008	Cost and Schedule Milestone Plan	6.1.1	ONE/R	NLT 10 DATO
A009	Contractor CPARS Draft Approval Document (CDAD) Report	6.1.1	MTHLY	30 DATO and on the 10th
A011	Cyber Security Workforce (CSWF) Report	6.1.1	MTHLY	NLT 10 DATO award and monthly on the 10th
A012	Provide INS Reporting - Tier III Meetings	6.2.1	WEEKLY	Weekly - as required.

12.1.2 Technical CDRL

See Exhibit A CDRLs attached to this task order. The following table lists all required technical data deliverables applicable to this task:

CDRL #	Deliverable Title	TO PWS Reference Para 6.#	Frequency	Date Due
A003	Task Order Status Report	6.1.1	MTHLY	30 Days after task order (DATO) and monthly on the 10th

A004	Contractor Manpower Quarterly Status Report	6.1.1	QRTLY	15 Jan, 15 Apr, 15 Jul, & 15 Oct
A005	Task Order Closeout Report	6.1.1	ONE	NLT 30 days after completion date
A008	Cost and Schedule Milestone Plan	6.1.1	ONE/R	NLT 10 DATO
A009	Contractor CPARS Draft Approval Document (CDAD) Report	6.1.1	MTHLY	30 DATO and on the 10th
A011	Cyber Security Workforce (CSWF) Report	6.1.1	MTHLY	NLT 10 DATO award and monthly on the 10th
A012	Provide INS Reporting - Tier III Meetings	6.2.1	WEEKLY	Weekly - as required.
T001	Enterprise-wide Contractor manpower reporting application (eCMRA) input	6.1.1.	ANNLY	NLT 31 Oct of each calendar year
T002	Invoice Support Documentation	6.1.1.	MTHLY	NLT 10 DATO and R/ on the 10th
T003	Limitation Notification & Rationale	6.1.1	ASREQ	Within 24 hrs from occurrence
T004	Vulnerability Assessment Requirement	6.4.1	ASREQ	Within 24 hrs from occurrence

12.2   NON-DATA DELIVERABLES

The following table lists all required non-data deliverables

#	Deliverable Title	TO PWS Reference Para 6.#	Frequency	Date Due
ND-1	Attendance - Tier III Meetings	6.2.1	Weekly	Weekly- as required

13.0   SUBCONTRACTING REQUIREMENTS

[(b)(4)] are approved to work on this task order.

14.0   ACCEPTANCE PLAN

Inspection and acceptance is performed by the COR on all services, data, and non-data deliverables in accordance with the Quality Assurance Surveillance Plan (QASP), Attachment 1.

15.0   OTHER CONDITIONS/REQUIREMENTS

15.1   QUALITY

The Contractor shall have processes in place that shall coincide with the Government's quality management processes. As required, the Contractor shall use best industry practices including, when applicable, ISO/IEC 15288 for System life cycle processes and ISO/IEC 12207 for Software life cycle processes. The Contractor shall provide technical program and project management support that will mitigate the risks to successful program execution including employment of Lean Six Sigma methodologies in compliance with SSC Atlantic requirements and with the SSC Engineering Process Office (EPO) Capability Maturity Model Integration (CMMI) program. As part of a team, the Contractor shall support projects at SSC Atlantic that are currently, or in the process of, being assessed under the SSC EPO CMMI program. The Contractor shall be required to utilize the processes and procedures already established for the project and the SSC EPO CMMI program and deliver products that are compliant with the aforementioned processes and procedures.

15.2   GOVERNMENT FACILITIES

Government facilities (i.e., office space, computer hardware/software, or lab space) will be provided to those labor categories (see pricing model estimated hours) that would otherwise adversely affect the work performance if they were not available on-site. All Contractor personnel with supplied government facilities shall be located at Marine Corps Base in Quantico, VA. Work under this order will be performed during normal working hours when practical.

15.3   PESONNEL QUALIFICATION SPECIFICATIONS

For all required personnel qualifications, a minimum of 50% of the personnel will have the qualifications at time of the award, and the remaining 50% must all meet the qualifications no later than 6 months after award of task order.

Experience shall be recent, having occurred within the last three years. For example: 5 years' experience required having occurred within the last 7 years.

Labor Category	Qualifications
EDM Active Directory (AD) Support SME (SME 4)	Education: a) Bachelor's degree in Computer Science or other related IT degree preferred. b) Expert level Professional series Certification within the Product Group (PG) technology scope (e.g. MCM, MCSE, MCITP, VCDX) Basic Experience: At least 3 years' experience working with VMWare Enterprise level based virtualization. Specialized Experience: At least 5 years' experience required in Active Directory support. IAT Level 3.
EDM Messaging Support SME (SME 4)	Education: a) Bachelor's degree in Computer Science or other related IT degree preferred. b) Expert level Professional series Certification within the PG technology scope (e.g. MCM, MCSE, MCITP, VCDX) Basic Experience: At least 3 years' experience working with VMWare Enterprise level based virtualization. Specialized Experience: At least 5 years' experience required in Active Directory and Exchange support. IAT Level 3.
EDM Virtualization Support SME (SME 4)	Education: a) Bachelor's degree in Computer Science or other related IT degree preferred. b) Expert level Professional series Certification within the PG technology scope (e.g. MCM, MCSE, MCITP, VCDX)

	Basic Experience: At least 3 years' experience working with Microsoft Servers. Specialized Experience: At least 5 years' experience required in VMWare's enterprise engineering and architecture support. IAT Level 3.
EDM Storage Area Network (SAN) Support (SME 4)	Education: a) Bachelor's degree in Computer Science or other related IT degree preferred. b) Expert level Professional series Certification within the PG technology scope (e.g. NCIE, EMCSA, EMCCA, EMCTA, or related.) Basic Experience: At least 3 years' experience working with Microsoft Servers. Specialized Experience: At least 5 years' experience required in VMWare s enterprise support. At least 5 years' experience required in SAN engineering and support. IAT Level 3.
EDM Event Management Support (SME 4)	Education: a) Bachelor's degree in Computer Science or other related IT degree preferred. b) Expert level Professional series Certification within the PG technology scope (e.g. MCM, MCSE, MCITP.) Specialized Experience: At least 5 years' experience required in Microsoft SCOM or MOM, ISA/TMG Server. IAT Level 3.
EDM Database Support (SME 4)	Education: a) Bachelor's degree in Computer Science or other related IT degree preferred. b) Expert level Professional series Certification within the PG technology scope (e.g. MCM, MCSE, MCITP, MCDBA.) Specialized Experience: At least 5 years' experience required in supporting Microsoft Database technology. IAT Level 3.
Integrated Network Support (SME 4)	Education: a) Bachelor's degree in Computer Science or other related IT degree preferred. b) Expert level Professional series

	Certification within the PG technology scope. c) Specialized Experience: IAT III, IAM III, IASAE II and/or CND-IS. Experience with BlueCoat preferred.
MCEN Event Management System (MEMS) Support (SME 4)	Education: a) Bachelor's degree in Computer Science or other related IT degree preferred. b) Expert level Professional series Certification within the PG technology scope (e.g. HP BSM, UCMDB, OMW, NNMi, HP SiteScope, HP Universal Discovery, HP SHR, HP SHA, HP SHO, HP RUM, HP Diagnostics Commander, HP SA, HP OO, and HP NA). Specialized Experience: 10 years working experience operating, designing HP event management tools in a robust enterprise environment. Specializing in: · HP Business Service Management (BSM) 9.22 · HP Universal Configuration Management Database (UCMDB) 10.01 · HP Operations Manager (OMW) (includes HP Performance Manager 9.00) 9.00 · HP Network Node Manager i (NNMi) (including I Smart Plug-in (iSPI) for Performance Metrics) 9.24 · HP SiteScope 11.22 · HP Universal Discovery 10.01 · HP Service Health Reporter (SHR) 9.30 · HP Service Health Analyzer (SHA) 9.30 · HP Service Health Optimizer (SHO) 9.30 · HP Real User Monitor Engine (RUM) 9.22 · HP Diagnostics Commander 9.22 · HP Server Automation (SA) 10.01 · HP Operations Orchestration (OO) 9.07 · HP Network Automation (NA) 9.22

	IAM Level 3. Expertise required for software versions listed and/or newer versions of these software tools in an enterprise environment. The environment consists of multiple instantiations of these systems in support of the unclassified, classified, and testing/integrations networks. These positions require extensive experience architecting and implementing solutions using the identified tools. Candidates must have extensive knowledge of and experience using and integrating these tools in regionalized Wide Area Networks (WANs) in large-scale, global, environments.
MCEN Migration Compliance and Quality Assurance Support SME (SME 4)	Bachelor's degree required. Overall three years of experience in assessing, analyzing, evaluating, validating, certifying and accrediting, etc., various businesses, systems, software development processes, etc., relative to one or more compliance standard, security controls/requirements, etc.. Experience • 2 years' experience in security test and evaluation (ST&E) • 3 years' experience in systems security evaluation • 2 years of policy and directive writing skills • 3 years Systems Security Engineering • Knowledge of DOD 8500 series • Experience with DIACAP • Experience with Risk Management Framework • DOD 8570 IAM level III certification • Experience using and analyzing results of security, system auditing tools. 1. MCCAST (NIPR/SIPR) 2. Remedy (NIPR/SIPR) 3. SNAP (NIPR/SIPR) 4. Win2K8R2 5. SQL2K8/12 6. Retina/ACAS 7. VMWare

	8. MS Office products
	9. SharePoint
	10. Linux
	11. CISCO
	12. Juniper
Program Manager (IT Project Management)	Education: Bachelor's Degree (technical major preferred) with 10 years of relevant work experience and professional certifications. Experience with IT and/or telecommunications project management, including service provisioning (requirements gathering, engineering, and implementation) and certification and accreditation.

15.4   KEY PERSONNEL

No key personnel on this task order.

15.5   OVERTIME HOURS

Overtime is expected for certain staff positions, and is estimate below.

Labor Categories	Overtime
MCEN Event Management System (MEMS) Support	*Not to exceed* **600 hours** in a given year total.

Core hours are 0700-1700 for MEMS support personnel, with on-call 24 hour support (regular 8 hr days are expected to occur within these hours; on call is defined as being able to offer support as needed via blackberry/phone /laptop; on call support for priority 1 issues and/or classified systems may require on-site work performance).

15.6   NON-DISCLOSURE AGREEMENT (NDA) REQUIREMENTS

In the course of performing this TO, the Contractor may be or has been given access to and/or entrusted with various forms of information or data from a wide variety of sources which the Contractor would not otherwise be entitled to be in possession of. Contractors shall submit a completed "Conflict of Interest and Non-Disclosure Statement" form for every employee working on the contract and appropriate corporate officer on behalf of the corporation.

As a condition to receiving access to the data, the Contractor shall:

·   Prior to having access to proprietary data, obtain the agreement of the applicable person or entity to permit access by the Contractor to such data.

·   Use the data solely for the purpose of performing duties under this contract.

·   Not discuss with, disclose, release, reproduce or otherwise provide or make available the data, or any portion thereof, to any employee of the Contractor unless and until each person has executed a copy of the individual non-disclosure agreement.

·   Not discuss with, disclose, release, reproduce or otherwise provide or make available the data, or any portion thereof, to any non-government person or entity including any subcontractor, joint venture, affiliate, successor or assignee of the Contractor, unless the KO (and any Contractor claiming the data is proprietary) have given prior written approval, and the person receiving the data has executed an individual non-disclosure agreement.

·   Establish safeguards to protect such data or software from unauthorized use or disclosure.

·   Indoctrinate its personnel who will have access to the data as to the restrictions under which access is granted. Any other use, disclosure, release or reproduction is unauthorized and may result in substantial criminal, civil and/or administrative penalties to the Contractor or to the individual who violates this special contract requirement or non-disclosure agreement.

·   Appropriate restrictive legends will be included by the Contractor on any copies and reproductions made of all or any part of the data and any data that is derived from, based upon, incorporate, include or refer to the data. When the Contractor's need for such data ends, the data shall be returned promptly (within ten (10) business days) to the appropriate government program personnel. However, the obligation not to discuss, disclose, release, reproduce or otherwise provide or make available such data, or any portion thereof, shall continue, even after completion of this contract/order. Any actual or suspected unauthorized use, disclosure, release, or reproduction of such data or violation of this agreement, of which the company or any employee is or may become aware, will be reported promptly (within one (1) business day) to the Contractor's program manager, who will inform the KO within five (5) business days of receiving the report.

16.0   LIST OF ATTACHMENTS

Attachment 1 – Quality Assurance Surveillance Plan (QASP)

Exhibit A - CDRLs

Table 1 – Acronyms

Acronym	Definition
AD	Active Directory
C&a	Certification & Accreditation
CDRL	Contract Data Requirements List
COR	Contracting Officer's Representative
CMMI	Capability Maturity Model Integration
CQA	Compliance and Quality Assurance
CSWF	Cyber Security Workforce
DCO	Defense Connect Online
DBA	Database
DCOS	Defense Cyber Operations Section
DISN	DISN Defense Information System Network
DOD	Department of Defense
DODN	Defense (DoD) Information Network
EDM	Enterprise Directory and Messaging
EPO	Engineering Process Office
FAQs	Frequently Asked Questions
FCL	Facility Security Clearance
FISMA	Federal Information Security Management Act
FY	Fiscal Year
FOBs	Forward Oeprating Bases
GFE	Government Furnished Equipment
GFF	Government-Furnished Facilities
GFI	Government-Furnished Information
GFP	Government-Furnished Property

IA	Information Assurance
IDNX	Integrated Digital Network Exchange
INS	Integrated Network Support
IS	Information Security
IT	Information Technology
LUNS	Logical Unit Numbers
MARFOR	Marine Corps Force
MCB	Marine Corps Base
MCEITS	Marine Corps Enterprise Information Technology Services
MCEN	Unified Marine Corps Enterprise Network
MCEN-N	Marine Corps Enterprise Network
MEMS	MCEN Event Management System
MCNOSC	Marine Corps Network Operations and Security Center
NACLC	National Agency Check with Local Agency Check and Credit Check
NDA	Non Disclosure Agreement
MOM	Microsoft Operations Manager
MTTR	Mean Time To Repair
NTE	Not to Exceed
NIPR	Non-secure Internet Protocol Routed Network
OEM	Original Equipment Manufacturer
PM	Project Manager
PG	Product Groups
POA&M	Plan of Action and Milestones
PWS	Performance Work Statement
QASP	Quality Assurance Surveillance Plan
RFC	Request for Change
RUM	Real User Monitoring
SA	Situational Awareness
SA	Server Automation
SAN	Storage Area NetworK
SNA	System Network Architectur
SCIF	SCI Facility
SCOM	Systems center Operations Manager
SHA	Service Intelligence Analyze
SIPR	SIPRNET
SNA	System Network Architecture
SOPs	Standard Operating Procedures
ST&E	Security Test and Evaluation
TBEC	Topology Based Event Correlation
TCP/IP	Transmission Control Protocol/Internet Protocol
TCO	Total Cost Of Ownership
USMC	United States Marine Corps
VOIP	Voice Over Internet Protocol
VOSIP	Voice Over Secure Internet Protocol
VTC	Video Teleconferencing
WAN	Wide Area Networks
WBS	Work Breakdown Structure

SECTION D PACKAGING AND MARKING

All Deliverables shall be packaged and marked IAW Best Commercial Practice.

SECTION E INSPECTION AND ACCEPTANCE

CLIN	INSPECT AT	INSPECT BY	ACCEPT AT	ACCEPT BY
1001	Destination	Government	Destination	Government
2001	Destination	Government	Destination	Government

SECTION F DELIVERABLES OR PERFORMANCE

The periods of performance for the following Items are as follows:

1001   9/30/2014 - 9/29/2015

CLIN - DELIVERIES OR PERFORMANCE

The period of performance for CLIN 2001 is as follows:

CLIN 2001: Begins after CLIN 0001 is complete and ends 365 days after CLIN 2001 is exercised.

SECTION G CONTRACT ADMINISTRATION DATA

5252.232-9208 INVOICING INSTRUCTIONS FOR SERVICES USING WIDE AREA WORK FLOW (WAWF) (APR 2009)

(a) Invoices for services rendered under this contract shall be submitted electronically through the Wide Area Work Flow-Receipt and Acceptance (WAWF). The contractor shall submit invoices for payment per contract terms. The Government shall process invoices for payment per contract terms.

(b) The vendor shall have their Cage Code activated by calling 1-866-618-5988 and selecting option 2. Once activated, the vendor shall self-register at the WAWF website at https://wawf.eb.mil. Vendor training is available on the internet at https://wawftraining.eb.mil. WAWF Vendor "Quick Reference" Guides are located at the following web site: http://acquisition.navy.mil/rda/home/acquisition_one_source/ebusiness/don_ebusiness_solutions/wawf_overview /vendor_information

(c) Cost back-up documentation (such as delivery receipts, labor hours & material/travel costs etc.) shall be included and attached to the invoice in WAWF. Attachments created with any Microsoft Office product or Adobe (.pdf files) are attachable to the invoice in WAWF. The total size limit for files per invoice is 5 megabytes. A separate copy shall be sent to the COR.

(d) Contractors approved by DCAA for direct billing will not process vouchers through DCAA, but may submit directly to DFAS. Vendors MUST still provide a copy of the invoice and any applicable cost back-up documentation supporting payment to the Acceptor/Contracting Officer's Representative (COR) if applicable. Additionally, a copy of the invoice(s) and attachment(s) at time of submission in WAWF shall also be provided to each point of contact identified in section (g) of this clause by email. If the invoice and/or receiving report are delivered in the email as an attachment it must be provided as a .PDF, Microsoft Office product or other mutually agreed upon form between the Contracting Officer and vendor.

(e) A separate invoice will be prepared no more frequently than for every two weeks. Do not combine the payment claims for services provided under this contract.

(f) The following information is provided for completion and routing of the invoice in WAWF:

Cost Contract Supply/ Service WAWF Table

Invoice Type:	Cost Vouchers
Issue by:	N65236
Admin by:	DCMA S0107A
DCAA Auditor DoDAAC:	DCAA HAA010
Service Approver DoDAAC	DCMA S0107A
PAY DODAAC:	DFAS HQ0338
Acceptor e-mail:	(b)(6)

(g) After submitting the document(s) to WAWF, click on "Send More Email Notifications" and add the acceptor/receiver email addresses noted below in the email address blocks. The contractor shall, at a minimum, include the COR, Receiver, and Acceptor. This additional notification to the government is necessary to ensure that the acceptor/receiver is aware that the invoice documents have been submitted into WAWF: Send Additional Email Notification(s) to:

Name	Email	Phone	Role
(b)(6), 54530	See above	202-284-(b)(6)	COR

The contractor shall cite on each invoice/voucher, in addition to all other requirements of this contract/order, the contract line item number (CLIN); the contract subline item number (SLIN) and accounting classification reference number (ACRN) for the portion, or portions of work being billed as specified in the contract or delivery order. For each ACRN on the invoice/voucher, the contractor shall identify the amount being billed against that ACRN. Invoices shall be submitted in accordance with Wide Area Work Flow as annotated by the basic contract. The contractor will electronically submit his invoices using the Wide Area Workflow (WAWF) web site located at https://wawf.eb.mil.

The telephone number for assistance pertaining to Wide Area Work Flow is 800-559-9293.

DELIVERY ORDER LIMITATIONS OF COST/FUNDS (DEC 1999)

In accordance with the FAR Clause 52.232-20, "Limitation of Cost," or 52.232-22 "Limitation of Funds," the Government shall not be obligated to reimburse the Contractor for work performed, items delivered, or any costs incurred under orders issued under the resultant contract, except as authorized by the contracting officer. The cost factors utilized in determining the estimated costs under any order placed hereunder shall be the applicable rates current at the time of issuance of the task or delivery order, not to exceed, however, any ceilings established by the terms of this contract. If at any time 75% of either the estimated cost or estimated level of effort specified in the task or delivery order is reached and it appears that additional funds and/or level of effort is required to complete performance, the Contractor shall promptly notify the Ordering Officer in writing. Such notification shall include the cost and level of effort expended and that which will be required to complete performance. The Government shall have the right to modify the task or delivery order accordingly. If the Contractor exceeds the estimated costs authorized by task or delivery order placed hereunder, the Government will be responsible only for reimbursement of the cost and payment of fee in an amount up to that established by the task or delivery order. The total amount of all task or delivery orders issued shall not exceed the estimated costs and fixed fee or level of effort set forth in this contract.

252.204-0011 Contract-wide: Proration SEP 2009

The payment office shall make payment from each ACRN within the contract or order in the same proportion as the amount of funding currently unliquidated for each ACRN.

```
Accounting Data

SLINID    PR Number            Amount
--------  --------------------  --------------------
1001      130043165600004       4813805.95
LLA :
AA 1741106 1A1A 253 67925 067443 2D M30605 4RCCGWF00094
Standard Number: M3060514RC00094
NWA/JON: 100000952427 0010


BASE Funding 4813805.95
Cumulative Funding 4813805.95
```

SECTION J LIST OF ATTACHMENTS

Attachment 1 QASP

Exhibit A CDRLs